SUBSTITUTE SPECIFICATION

DEVICE FOR AUTHENTICATING DIGITAL IMAGES

OK TO ENTER SUBSTITUTE SPECIFICATION

FIELD OF THE INVENTION

The present invention relates to a device for authenticating digital images.

The invention applies more particularly to the authenticating of digital images emanating from a picture taking apparatus such as, for example, a camera head or a photographic apparatus.

BACKGROUND OF THE INVENTION

Digital images are falsifiable images. Thus are, for example, digital images constituting a news report or a television transmission, whether these images are broadcast live or from a source of recorded data.

People to whom digital images are sent therefore find themselves in a situation where the authenticity of the information which they receive is not guaranteed. This drawback is all the more significant with the proliferation of sources of information such as, for example, the sources of information originating from journalists commonly referred to as "freelance" journalists. To avoid this drawback, processes for authenticating digital images have been proposed, in particular in the patent US 5,499,294. These processes make it possible to authenticate the picture taking apparatus itself but not the journalist or the cameraman.

OK cm 12-11-03

The purpose of the invention is to remedy this drawback.

SUMMARY

The present invention relates to a device for authenticating the taking of pictures made up of digital data comprising a picture taking apparatus and a security element carrying out the signing of at least part of the digital data, characterized in that the security element is a detachable element comprising an encryption circuit with secret key K1, this element being connected to the picture taking apparatus by an interface circuit provided in the picture taking apparatus.

BRIEF DESCRIPTION OF THE DRAWINGS

Other advantages and characteristics of the invention will become apparent on reading a preferred embodiment given with reference to the hereto appended figures in which:

- Figure 1 represents a first picture taking device allowing the authentication of digital images according to the preferred embodiment of the invention;

- Figure 2 represents a second picture taking device allowing the authentication of digital images according to the preferred embodiment of the invention;

- Figure 3 represents, according to the invention, a device for authenticating the digital images emanating from a picture taking device such as that represented in Figure 1 or in Figure 2.

DETAILED DESCRIPTION OF THE INVENTION

In all the figures, the same labels designate the same elements.

Figure 1 represents a first picture taking device allowing the authentication of digital images according to the preferred embodiment of the invention.

The picture taking device consists of a picture taking apparatus 1 and of a detachable security element 2. The picture taking apparatus 1 can be, for example, a camera head or a photographic apparatus. According to the preferred embodiment of the invention, the detachable security element is a chip card.

The picture taking apparatus 1 comprises an objective 3, a block 4 of circuits for processing the signal emanating from the objective 3, a hashing circuit 5, a multiplexer 6 and a circuit 7 for interfacing with the chip card.

In a manner known per se, the objective 3 and the block 4 of processing circuits make it possible to transform a light signal L into a digital signal VN.

According to the invention, a fraction F1(VN) of the digital signal VN is tapped off, preferably in a regular manner, at the output of the block 4. Each fraction F1(VN) tapped off is sent to the hashing circuit 5. The circuit 5 can be an electronic circuit or a software element. By way of nonlimiting examples, the fraction F1(VN) of the digital signal VN can be made up of the even or odd lines of the same image or of the data relating to the luminance component of the same image. The fraction F1(VN) can also be made up of several frames tapped off at regular time intervals in the case of a camera head or image by image in the case of a photographic apparatus. In a general manner, the datum F1(VN) is made up of significant data of an image.

The result m1 emanating from the function for hashing the signal F1(VN) is sent to the interface circuit 7. The datum m1 comprises, for example, a few tens of bits.

The interface circuit 7 allows the bidirectional transfer of data between the apparatus 1 and the chip card 2. Preferably, the circuit 7 is a bidirectional serial interface circuit to the ISO-7816 standard.

The chip card contains an encryption circuit (not represented in the figure) as well as a secret key K1. Preferably, the key K1 is stored in a programmable memory contained in the card 2. Under the action of the key K1, the successive data m1 sent to the card 2 are encrypted by the encryption circuit so as to constitute a string of data $D(m1)_{K1}$. Each datum $D(m1)_{K1}$ constitutes the signature of the datum m1 and hence of the fraction F1(VN) from which the datum m1 emanated.

By way of the interface circuit 7, the data $D(m1)_{K1}$ are sent from the chip card 2 to a first input of the multiplexer 6 which receives, in addition, the digital signal VN on a second of its inputs.

The signal S1 emanating from the multiplexer 6 is then made up of the digital data VN and of the data $D(m1)_{K1}$. Preferably, each datum $D(m1)_{K1}$ is inserted into a header associated with the fraction of datum F1(VN) which corresponds thereto. According to another embodiment of the invention, the data $D(m1)_{K1}$ are substituted for some of the data VN which are then lost.

Figure 2 represents a second picture taking device allowing the authentication of digital images according to the preferred embodiment of the invention.

The picture taking device consists of a picture taking apparatus 8 and of a detachable security element 9, for example, a chip card. The apparatus 8 can be, for example, a

camera head or a photographic apparatus. The apparatus 8 contains the same circuits as the apparatus 1 described in Figure 1 with the exception of the hashing circuit 5.

According to the embodiment of Figure 2, the hashing function is carried out in the chip card 9. From this it follows that the fraction F1(VN) of the digital signal VN is sent to the chip card 9.

As mentioned hereinabove, the hashing of the datum F1(VN) generates a datum m1 which, encrypted, generates a datum $D(m1)_{K1}$. By way of the interface circuit 7 the successive data $D(m1)_{K1}$ are sent from the chip card 9 to the multiplexer 6. The signal S1 emanating from the picture taking apparatus 8 is then generated as mentioned earlier.

A picture taking device according to the invention operates with encryption keys K1 having different values. One and the same key K1 can then be specific to one person or to a set of people constituting, for example, a collection of journalists. From this it follows that an advantage of the invention is that it guarantees the origin of the authenticated images.

In accordance with the invention, the chip card provides for a personal key function whose key is secret. Moreover, the use of a chip card implies the implementation of a procedure of mutual identification between the chip card and the device receiving the chip card, namely the picture taking apparatus. From this it follows that the security level relating to the various steps implemented in the chip card and the picture taking device is a high security level.

Figure 3 represents, according to the invention, a device for authenticating digital images emanating from a picture taking device such as that represented in Figure 1 or in Figure 2.

The device 10 for authenticating digital images comprises a demultiplexer 11, a decryption circuit 12 with public key K2, a hashing circuit 13 and a comparator 14. The demultiplexer 11 receives on its input a signal S1 such as that mentioned in Figures 1 and 2. The signal S1 originates either from a picture taking device such as that described in Figures 1 and 2, or from a source of recorded data such as, for example, a magnetic tape, a digital video disc or else a diskette.

The function of the demultiplexer 11 is to separate the data $D(m1)_{K1}$ from the digital data VN. The data $D(m1)_{K1}$ are sent to the decryption circuit 12 with public key K2.

The operation of decryption with public key K2 of a datum $D(m1)_{K1}$ leads to the calculation of a decrypted datum $C(D(m1)_{K1})_{K2}$.

According to the invention, fractions F2(VN) of the digital signal VN are tapped off at the output of the demultiplexer 11. The tapping off of the fractions F2(VN) is performed as a mirror image of the tapping off of the fractions F1(VN). Thus, each fraction F2(VN) corresponds to a fraction F1(VN) and the data which are contained in the fraction F2(VN) which corresponds to the fraction F1(VN) are data of the same type as the data contained in the fraction F1(VN). The expression "data of the same type" should be understood to mean that the data which constitute the fraction F2(VN) are data which are a priori identical to the data which constitute the fraction F1(VN) which corresponds thereto: the data are identical if the fraction F1(VN) has not been falsified and different, in whole or in part, if the fraction F1(VN) has been falsified.

In all cases, the data contained in a fraction F2(VN) represent the same signal as the data contained in the fraction F1(VN) corresponding thereto. Thus, for example, if the data

contained in a fraction F1(VN) are made up of the even lines of an image, the data contained in the fraction F2(VN) which corresponds to the fraction F1(VN) are made up of the even lines of the same image.

The circuit 13 operates the hashing of the data contained in the fractions F2(VN). The hashing operation performed by the circuit 13 is identical to that performed by the circuit 5. From this it follows that the datum m2 which is associated with a fraction F2(VN) corresponding to a fraction F1(VN) is identical to the datum m1 which is associated with the fraction F1(VN) if the fraction F1(VN) has not been falsified. The datum m2 emanating from the circuit 13 and the datum $C(D(m1)_{K1})_{K2}$ are sent to the comparator 14.

The signal S3 emanating from the comparator 14 then makes it possible to indicate whether the digital data VN are authentic data or falsified data: these are data which can be regarded as authentic if each datum m2 is equal to the datum $C(D(m1)_{K1})_{K2}$ corresponding thereto, these are data where one is aware that they have been falsified if at least one datum m2 is different from the datum $C(D(m1)_{K1})_{K2}$ corresponding thereto.

According to the invention, the device 10 for authenticating images can be incorporated into a control unit receiving images filmed by a camera head.

PTN\38103.1